Vypočítateľnosť - nezaradené

1. Funkcie a čiastočné funkcie, projekcie, skladanie funkcií, trojice číslovacích (párovacích) funkcií.

Príklad. Extencionálnosť: Je rozdiel medzi funkciou a spôsobom jej zadania. Algoritmickú funkciu nemusíme zadať algoritmom, teda vieme mať zadanú funkciu ale nevedieť čo počíta. Preto sa budeme viac zaoberať zadaním.

$f(x) = 1$ ak v desiatkovom rozvoji čísla Π je presne x číslic 5 idúcich za sebou. Ináč $f(x) = 0$. Doteraz nikto nezistil, či existuje algoritmus, čo počíta túto funkciu.

$g(x) = 1$ ak v desiatkovom rozvoji Π je aspoň x číslic 5 idúcich za sebou. 0 ináč. Táto funkcia je "monotónna" – najskôr je to jedna, a potom nula alebo je to stále jedna. V oboch prípadoch je to to vypočítateľná funkcia (iba jeden if, alebo iba výpis 1). Ale neviem algoritmus

Poznámka. Extencionálnosť znamená, že funkcia môže mať rôzne zadania.

tzv. Churchova λ-notácia.

Označenie 1.26. Nech $F(x_1, \ldots, x_n)$ je výraz, ktorý pri dosadení ľubovoľných prvkov z množiny X za $x_1, \ldots, x_n$ je nedefinovaný, alebo má hodnotu z množiny X. Potom znakom

$$\lambda_X x_1 \ldots x_n F(x_1, \ldots, x_n)$$

označíme takú n-árnu čiastočnú funkciu f na množine X, že pre všetky $a_1, \ldots, a_n \in X$ platí

$$f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$$

Pokiaľ nebude hroziť nedorozumenie, budeme index pri písmene λ vynechávať.

Príklad. Churchova λ notácia pre funkcie $N^k \to N$:

- $\lambda xy\ (5x + y)$
- $\lambda xyz\ (5x + y)$, z je fiktívna premenná.
- $\lambda y\ (5x + y)$, x je parameter opisujúci množinu funkcií
- $\lambda y\ (10)$ – unárna konštanta.
- $\lambda\ (10)$ – nulárna konštanta.
- $\lambda\ (x+1) = s(x)$
- $\lambda xy\ (x^3 + y) = \lambda yx\ (y^3 + x)$
- $\lambda xy\ (x^3 + y) \neq \lambda xy\ (y^3 + x)$

Úvod ku číslovacím funkciám:

Definícia 3.41. Nech pre všetky $x_1, y_1, x_2, y_2 \in \mathbb{N}$ je $(x_1, y_1) \prec (x_2, y_2)$ práve vtedy, keď $x_1 + y_1 < x_2 + y_2$ alebo $x_1 + y_1 = x_2 + y_2$ a $x_1 < x_2$.

Teraz môžeme podľa tohto usporiadania zoradiť všetky prvky množiny $\mathbb{N} \times \mathbb{N}$ do prostej postupnosti

$$(0,0), \quad (0,1), \quad (1,0), \quad (0,2), \quad (1,1), \quad (2,0), \quad \ldots \qquad (3.41.1)$$

a definovať:

Definícia 3.42.

$$\begin{aligned} \mathrm{c}(x,y) &= \text{číslo člena } (x,y) \text{ v postupnosti } (3.41.1) \\ \mathrm{l}(x) &= \text{prvý prvok dvojice na } x\text{-tom mieste postupnosti } (3.41.1) \\ \mathrm{r}(x) &= \text{druhý prvok dvojice na } x\text{-tom mieste postupnosti } (3.41.1) \end{aligned}$$

Teda

$$\begin{aligned} \mathrm{c}(0,0) &= 0, & \mathrm{c}(0,1) &= 1, & \mathrm{c}(1,0) &= 2, & \ldots \\ \mathrm{l}(0) &= 0, & \mathrm{l}(1) &= 0, & \mathrm{l}(2) &= 1, & \ldots \\ \mathrm{r}(0) &= 0, & \mathrm{r}(1) &= 1, & \mathrm{r}(2) &= 0, & \ldots \end{aligned}$$

Príklad ku číslovacím funkciám:

Príklad 3.63. Dokážeme niekoľkými spôsobmi primitívnu rekurzívnosť funkcie $f(x)$ danej predpisom

$$f(0) = 0, \qquad f(1) = 1, \qquad f(x+2) = f(x+1) + f(x),$$

t.j. Fibbonaciho postupnosti.

(a) Dokážeme najprv primitívnu rekurzívnosť funkcie $g(x) = \mathrm{c}(f(x), f(x+1))$. Platí

$$\begin{aligned} g(0) &= \mathrm{c}(0,1) = 1, \\ g(x+1) &= \mathrm{c}(f(x+1), f(x+2)) = \\ &= \mathrm{c}(f(x+1), f(x+1) + f(x)) = \\ &= \mathrm{c}(\mathrm{r}(g(x)), \mathrm{r}(g(x)) + \mathrm{l}(g(x))) \end{aligned}$$

Teda funkcia g je primitívne rekurzívna, lebo vzniká operáciou primitívnej rekurzie z primitívne rekurzívnych funkcií $\lambda(1)$, $\lambda xy(\mathrm{c}(\mathrm{r}(y), \mathrm{r}(y) + \mathrm{l}(y)))$.

(b) Môžeme postupovať rovnako ako v prípade (a), len zvoliť $g(x) = 2^{f(x)} \cdot 3^{f(x+1)}$ a používať funkcie $\mathrm{ex}_0(x)$, $\mathrm{ex}_1(x)$ namiesto funkcií $\mathrm{l}(x)$, $\mathrm{r}(x)$. (Nezáleží na tom, že z týchto funkcií nemožno vytvoriť trojicu číslovacích funkcií.)

(c) Dokážeme najprv primitívnu rekurzívnosť funkcie $h(x) = \mathrm{c}^{x+1}(f(0), f(1), \ldots, f(x))$. Pre $x \in \mathbb{N}$, $x \neq 0$ platí

$$\begin{aligned} f(x) &= \mathrm{r}(h(x)), \\ f(x-1) &= \mathrm{r}(\mathrm{l}(h(x))) \\ h(x+1) &= \mathrm{c}(h(x), \mathrm{r}(h(x)) + \mathrm{r}(\mathrm{l}(h(x)))) \end{aligned}$$

Tento vzťah upravíme tak, aby platil aj pre $x = 0$:

$$h(x+1) = \mathrm{c}(h(x), \mathrm{r}(h(x)) + \mathrm{r}(\mathrm{l}(h(x)))) + \overline{\mathrm{sg}}(x)$$

Posledný vzťah spolu so vzťahom $h(0) = 0$ definuje funkciu h primitívnou rekurziou z primitívne rekurzívnych funkcií. Teda funkcia h, a potom aj funkcia $f(x) = \mathrm{r}(h(x))$ je primitívne rekurzívna.

(d) Namiesto funkcie h z bodu (c) možno použiť funkciu

$$h(x) = \mathrm{p}_0^{f(0)} \cdot \mathrm{p}_1^{f(1)} \cdots \mathrm{p}_x^{f(x)}$$

Funkcia f sa dá vyjadriť pomocou funkcie h takto:

$$f(x) = \mathrm{ex}(\mathrm{npr}(h(x)) \dot{-} 1, h(x))$$

2. Univerzálne funkcie a čiastočné funkcie. + univerzálne množiny

Cvičenie. Existuje rekurzívna množina $R \subseteq \mathbb{N} \times \mathbb{N}$, ktorá je univerzálna pre triedu všetkých rekurzívnych podmnožín $\mathbb{N}$?

Riešenie. Nech existuje. M je rekurzívna, ak jej χ_M je vypočítateľná. Rekurzívnych množín je nekonečne veľa.

	0	1	2	3	4
χ_{M_0}	0	1	1	1	0
χ_{M_1}	0	1	1	1	0
$\dots$					
χ_{M_i}	0	1	1	1	0

Zoberiem diagonálu, tam to znegujem $\chi(x) = 1 - \chi_x(x)$ Táto tam nepatrí, ale je rekurzívne spočítateľná.

Cvičenie. Ukážte, že ani $U(n, n)$ nemá vypočítateľné zúplnenie.

Riešenie. Ak $U(n, n)$ nie je vypočítateľné zúplnenie, potom $U(n, n) + 1$ nie je vypočítateľné zuplnenie.

Poznámka. Funkcia $d(n) = U(n, n)$ nemá vypočítateľné zúplnenie. Preto jej definičný obor je množina, ktorá je rekurzívne očíslovateľná, ale nie je rekurzívna. Podľa Postovej vety, to znamená, že doplnok k jej definičnému oboru nie je rekurzívne očíslovateľný (komplement $Arg(U(n, n))$ nie je rekurzívne očíslovateľný). Z toho vyplýva, že definičný obor celej U je rekurzívne očíslovateľný. Z toho vyplýva, že doplnok k $Arg(U(n, x))$ nie je rekurzívne očíslovateľný.

Problém zastavenia turingovho stroja nie je algoritmicky riešiteľný.

Priamy ťah na bránku: Máme formalizáciu pojmu algoritmus. Prvá podmienka je, že chceme vedieť o texte rozhodnúť, či daný text opisuje program, alebo nie. Chceme číslovanie programov $(p_0, p_1, \dots)$, číslovanie funkcií $\mathbb{N} \to \mathbb{N}$, univerzálnu funkciu $U(n, x)$, diagonála $U(n, n)$ nemá vypočítateľné zúplnenie. A teda $Arg(U(n, n))$ je rekurzívne očíslovateľná množina, ktorá nie je rekurzívna množina.

3. Primitívne rekurzívne, rekurzívne funkcie a čiastočne rekurzívne (vypočítateľné) funkcie (na množine N).

Programátorská poznámka ku primitívnej rekurzii: pamäť obsahuje n+2 hodnôt (y, f(y, $\bar{x}$), $\bar{x}$)

```
P {k, x̄ ∈ N^(n+1)}
F := h( x̄ );
Y := 0;
While Y < k do begin
        F := g(Y,F, x̄ );
        Y := s(Y);
End {F:=f(k, x̄ )}
```

Poznámka. Primitívne rekurzívne funkcie sú totálne. Tvrdenie dokazujeme indukciou vzhľadom na zostrojenie, všetky základné operácie (0,s,I,S,R) zachovávajú totálnosť.

Poznámka ku vete 5.0.3. Veta umožňuje meniť poradie premenných, stotožňovať premenné (k_i=k_j) a pridávať fiktívne premenné (m<n)

Príklad. Nech $\lambda xy(x^y) \in M$
$\lambda x(x^x) \in M$. – stotožnenie premenných.
$\lambda xyz(x^y) \in M$. – dodanie fiktívnej premennej.
$\lambda xz(x^x) \in M$.
$\lambda x, y(y^n) \in M$. – permutácia premenných.

Príklady na primitívne rekurzívne funkcie

Veta 3.12. Funkcie

$$\mathrm{sg}(x) = \begin{cases} 0, & \text{ak } x = 0 \\ 1, & \text{ak } x \neq 0 \end{cases}$$

$$\overline{\mathrm{sg}}(x) = 1 - \mathrm{sg}(x)$$

sú primitívne rekurzívne.
Dôkaz: Tieto funkcie vznikajú primitívnou rekurziou z konštantných funkcií, napríklad

$$\mathrm{sg}(0) = 0$$
$$\mathrm{sg}(x+1) = 1$$

a preto sú primitívne rekurzívne. □

Lema 3.13. Funkcia

$$x \dot{-} 1 = \begin{cases} 0, & \text{ak } x = 0 \\ x - 1 & \text{ak } x \neq 0 \end{cases}$$

je primitívne rekurzívna.
Dôkaz: Funkcie 0, I_1^2 sú primitívne rekurzívne a platí

$$0 \dot{-} 1 = 0$$
$$(x+1) \dot{-} 1 = I_1^2(x, x \dot{-} 1)$$

Tým je lema dokázaná. □

Veta 3.14. Funkcie

$$x \dot{-} y = \begin{cases} 0, & \text{ak } x < y \\ x - y, & \text{ak } x \geq y \end{cases}$$

$$|x - y| = (x \dot{-} y) + (y \dot{-} x)$$

sú primitívne rekurzívne.
Dôkaz: Pre prvú funkciu stačí uvážiť vzťahy

$$x \dot{-} 0 = x$$
$$x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1$$

Primitívna rekurzívnosť funkcie $|x - y|$ vyplýva teraz už bezprostredne z jej definície. □

Poznámka. 1. A = B → sg(|A − B|) = 0 , $\overline{Sg}$(|A − B|) = 1

2. A ≠ B → sg(|A − B|) = 1, $\overline{Sg}$(|A − B|) = 0

3. A ≤ B → sg(A $\dot{-}$ B) = 0, $\overline{Sg}$(|A $\dot{-}$ B|) = 1

4. A > B → sg(A $\dot{-}$ B) = 1, $\overline{Sg}$(|A $\dot{-}$ B|) = 0

5. A < B → sg(B $\dot{-}$ A) = 1, $\overline{Sg}$(|B $\dot{-}$ A|) = 0

Príklady na primitívne rekurzívne funkcie so sumami alebo súčinmi:

Veta 3.29. Funkcia

$$x \text{ MOD } y = \begin{cases} \text{zvyšok pri delení } x/y, & \text{ak } y \neq 0, \\ x, & \text{ak } y = 0 \end{cases}$$

je primitívne rekurzívna.

Dôkaz: Platí $x \text{ MOD } y = x \dot{-} y.\lfloor x/y \rfloor$, a teda fukcia MOD je primitívne rekurzívna, lebo vzniká skladaním z primitívne rekurzívnych funkcií. □

Veta 3.30. Funkcie

$$\text{div}(x, y) = \begin{cases} 1, & \text{ak } y \text{ je deliteľom } x \text{ (t.j. } y|x\text{)}, \\ 0, & \text{ak } y \text{ nie je deliteľom } x \text{ (t.j. } y \nmid x\text{)} \end{cases}$$

$$\text{nd}(x) = \begin{cases} \text{počet (kladných) deliteľov } x, & \text{ak } x \neq 0, \\ 0, & \text{ak } x = 0 \end{cases}$$

sú primitívne rekurzívne.

Dôkaz: Veta vyplýva bezprostredne zo vzťahov

$$\text{div}(x, y) = \overline{\text{sg}}(x \text{ MOD } y)), \quad \text{nd}(x) = \sum_{i=1}^{x} \text{div}(x, i) \quad \square$$

Veta 3.32. Funkcie

$$\chi_p(x) = \begin{cases} 0, & \text{ak } x \text{ je prvočíslo}, \\ 1, & \text{ak } x \text{ nie je prvočíslo}, \end{cases}$$

$$\pi(x) = \text{počet prvočísel menších alebo rovnajúcich sa } x$$

sú primitívne rekurzívne.

Dôkaz: Prvočísla sú čísla, ktoré majú práve dva kladné delitele, a preto platí

$$\chi_p(x) = \text{sg}\,|\,\text{nd}(x) - 2|$$

Pre funkciu $\pi(x)$ zrejme platí

$$\pi(x) = \sum_{i=0}^{x} \overline{\text{sg}}(\chi_p(i))$$

Z uvedených vyjadrení vyplýva, že funkcie $\chi_p(x)$, $\pi(x)$ sú primitívne rekurzívne. □

Príklady na primitívne rekurzívne funkcie s minimalizáciou:

Veta 3.33. Funkcia

$$\text{p}(x) = x\text{-té prvočíslo},$$

t.j. $\text{p}(0) = 2$, $\text{p}(1) = 3$, $\text{p}(2) = 5$, ... je primitívne rekurzívna.

Dôkaz: Platí

$$\text{p}(x) = \mu_y(|\pi(y) - (x+1)| = 0)$$

teda funkcia $\text{p}(x)$ vzniká z funkcie $\lambda yx|\pi(y) - (x+1)|$ minimalizáciou. Matematickou indukciou sa dá dokázať, že platí

$$\text{p}(x) \leq 2^{2^x}$$

Funkcia 2^{2^x} je primitívne rekurzívna, a preto podľa vety 3.26 aj funkcia $\text{p}(x)$ je primitívne rekurzívna. □

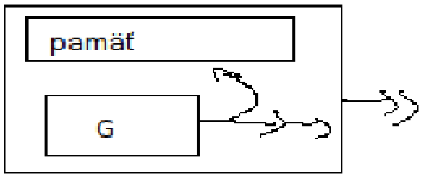
4. Primitívne rekurzívne, rekurzívne a rekurzívne spočítateľné množiny a predikáty a ich vlastnosti.

Príklad. Existuje nerekurzívna množina $M \subset \mathbb{N}$.

Príklad. Množina dvojíc $(n, n^2), n \in \mathbb{N}$ a n je nepárne je rekurzívne očíslovateľná.

```
x:=0;
while true do
    if (x mod 2=1) then write((x, x^2))
    x:=x+1
```

Odstránenie opakovania tlače zabezpečíme pamäťou. Budeme si pamätať čo už sme vytlačili a pri každom tlačení pozrieme do pamäte a vytlačíme prvok, ak sa v pamäti nenachádza.



Cvičenie. Nech $F \subseteq \mathbb{N} \times \mathbb{N}$ je rekurzívne očíslovateľná množina (neprázdna). Ukážte, že existuje vypočítateľná funkcia $f : \mathbb{N} \to \mathbb{N}$ taká, že $f \subseteq F$ (s maximálnym definičným oborom)

Riešenie.

a) $f = \emptyset$ – nikde nie je definovaná (ale už so zmeneným zadaním je toto zle:-).

b) Máme generátor G množiny F. Ak vygeneruje (x, y), tak sa pozrem, či už som x vygeneroval, ak nie, tak vyhodím (x, y), a ináč si zapíšem x.

Cvičenie. Nech $M \subseteq \mathbb{N}$ je nekonečná, rekurzívne očíslovateľná množina. Ukážte, že existuje nekonečne veľa poradí, generovania M, takých, že pre ne existuje generátor.

Riešenie. Každý generátor bude mať parameter p. Generátor M_p funguje ako generátor (bez opakovania) množiny M, ale ak vypočíta p-ty výsledok, počká aj na $p+1$ výsledok a v poradí ich vymení. Alebo najskôr vypočíta prvých p a potom ich dá v opačnom poradí. Alebo dá p-ty ako prvý, prvý ako p-ty.

Cvičenie. Nech $F \subseteq \mathbb{N} \times \mathbb{N}$ je rekurzívne očíslovateľná množina (neprázdna). Ukážte, že existuje vypočítateľná funkcia $f : \mathbb{N} \to \mathbb{N}$ taká, že $f \subseteq F$ (s maximálnym definičným oborom)

Riešenie.

a) $f = \emptyset$ – nikde nie je definovaná (ale už so zmeneným zadaním je toto zle:-).

b) Máme generátor G množiny F. Ak vygeneruje (x, y), tak sa pozrem, či už som x vygeneroval, ak nie, tak vyhodím (x, y), a ináč si zapíšem x.

Cvičenie. Nech $M \subseteq \mathbb{N}$ je nekonečná, rekurzívne očíslovateľná množina. Ukážte, že existuje nekonečne veľa poradí, generovania M, takých, že pre ne existuje generátor.

Riešenie. Každý generátor bude mať parameter p. Generátor M_p funguje ako generátor (bez opakovania) množiny M, ale ak vypočíta p-ty výsledok, počká aj na $p+1$ výsledok a v poradí ich vymení. Alebo najskôr vypočíta prvých p a potom ich dá v opačnom poradí. Alebo dá p-ty ako prvý, prvý ako p-ty.

Cvičenie. Nech $M \subseteq \mathbb{N}, K \subseteq \mathbb{N}$ sú rekurzívne očíslovateľné s neprázdnym prienikom. Ukážte, že existujú podmnožiny $M' \subseteq M, K' \subseteq K$, ktoré sú rekurzívne očíslovateľné, ale $M' \cap K' = \emptyset$, ale $M' \cup K' = M \cup K$.

Riešenie. Generujeme M aj K. Ak príde skôr z M, tak ho vygeneruje M', ináč ho vygeneruje K'. *(spoločné prvky sú toho, kto ich skôr vygeneruje)*

Cvičenie. Ukážte, že každá rekurzívne očíslovateľná množina M sa dá zapísať v tvare očíslovanej postupnosti, pričom $f(0), f(1)$, pričom f je vypočítateľná a bez opakovania.

Riešenie. Máme generátor M, generujeme, vyhadzujeme duplikáty a pridávame poradie. Toto je vypočítateľné: dostaneme (x, y) a počkáme prvých x rôznych.

Cvičenie. Každá nekonečná rekurzívna očíslovateľná množina $M \subseteq \mathbb{N}$ obsahuje nekonečnú rekurzívnu podmnožinu.

Riešenie. M je nekonečná postupnosť – M obsahuje nekonečnú rastúcu podpostupnosť. Pamätáme si posledné maximum a ak príde väčší, tak ho vyhodíme. Je to rekurzívne – ak je maximum už väčšie ako vstup, tak viem, že ho už nevygenerujem.

Cvičenie. Ku každej vypočítateľnej funkcii jednej premennej existuje vypočítateľná funkcia g, ktorá (je "pseudoinverzia") spĺňa vlastnosti:

a) definičný obor g=obor hodnôt f

b) $f(g(f(x))) = f(x)$ pre všetky x z definičného oboru f.

Riešenie. Zoberiem (x, y) vyhodím (y, x), ale ak už také y bolo, tak nevyhodím.

Príklad. Nasledujúce množiny sú rekurzívne: N: if n∈ N then 1 = λ(1) else 0
∅: if n∈ ∅ then 1 = λ(0) else 0

Príklad primitívne rekurzívnych množín:

Príklad: $\chi_\emptyset(x) = 1 = \lambda x(1) \in PRF$
$\chi_{\mathbb{N}}(x) = 0 = \lambda x(0) \in PRF$

$\chi_{2\mathbb{N}}(x) = x \bmod 2$
$\chi_{2\mathbb{N}+1}(x) = \overline{sg}(x \bmod 2)$

$M = \{a_1 \ldots a_n\}$
$\chi_M(x) = sg(|x - a_1|$

$\chi_\leq(x,y) = sg(x \dot{-} y)$
$\chi_=(x,y) = sg(|x-y|)$
$\chi_\neq(x,y) = \overline{sg}(|x-y|)$
$\chi_<(x,y) = sg(|x+1| \dot{-} y)$

Lema 7.2.2 *a)* $ROM = \Sigma_1, VRM = \Sigma_1 \cap \Pi_1$

b) $A \in \Sigma_n \Leftrightarrow \bar{A} \in \Pi_n; a \in \Pi_n \Leftrightarrow \bar{A} \in \Sigma_n$.

c) Zjednotenie a prienik k-árnych Σ_n množín (relácii) je opäť Σ_n (relácia) množina. Zjednotenie a prienik k-árnych Π_n množín(relácii) je opäť Π_n (relácia) množina.

d) Σ_n podmienky aj Π_n podmienky sú uzavreté na ohraničenú kvantifikáciu.

e) Σ_n podmienky sú uzavreté na existenčnú kvantifikáciu a Π_n podmienky sú uzavreté na všeobecnú kvantifikáciu.

f) $\Sigma_n \cup \Pi_n \subseteq \Sigma_{n+1} \cap \Pi_{n+1}$.

g) ak $A \leq_m B$ a $B \in \Sigma_n$, potom aj $A \in \Sigma_n$.

h) ak $A \leq_m B$ a $B \in \Pi_n$, potom aj $A \in \Pi_n$.

D: (a) $ROM = \Sigma_1$ $\quad A \in ROM \Leftrightarrow A = \{\bar{x} \mid (\exists v_1) \underbrace{g(\bar{x}, v) = 0}_{VRF}\} \in \Sigma_1$

projekcia

$VRM = \underset{ROM}{\Sigma_1} \cap \underset{doplnok}{\Pi_1}$ $\quad$ postova veta

$\bar{A} = \{\bar{x} \mid \neg(\exists v_1) g(\bar{x}, v) = 0\}$

$= \{\bar{x} \mid (\forall v_1) \underbrace{\overline{sg}(g(\bar{x}, v)) = 0}_{VRF}\} \in \Pi_1$

$\Leftarrow$ opačná implikácia:

$A \in \Sigma_1 \cap \Pi_1 \Rightarrow VRF$

$$\left.\begin{array}{l} A \in \Sigma_1 \Rightarrow A \in ROM \\ A \in \Pi_1 \Rightarrow \bar{A} \in \Sigma_1 \Rightarrow \bar{A} \in ROM \end{array}\right\} \begin{array}{l} \text{Postova veta} \\ A \in VRF \end{array}$$

(b) $A \in \Sigma_m \Leftrightarrow \bar{A} \in \Pi_m$

$A \in \Sigma_m \Rightarrow A = \{x_1 .. x_k \mid (\exists v_1)(\forall v_2) .. (Q v_m) \underbrace{P(x_1 .. x_k, v_1 .. v_m)}_{g(x_1 .. x_k, v_1 .. v_m) = 0}\}$

$\bar{A} \in \Pi_m \Rightarrow \bar{A} = \{x_1 .. x_k \mid (\forall v_1)(\exists v_2) .. (Q v_m) \underbrace{\neg P(x_1 .. x_k, v_1 .. v_m)}_{\overline{sg}(g(x_1 .. x_k, v_1 .. v_m)) = 0}\}$

(f) $\Sigma_m \cup \Pi_m \subseteq \Sigma_{m+1} \cap \Pi_{m+1}$

do predikátu $P(x_1 .. x_m, v_1 .. v_m)$ zavedieme fiktívnu premennú, ale ten predikát bude počítať to isté, čo pôvodný P

v_{m+1} na nič ju nevyberie

$A \in \Sigma_{m+1}$ $\quad A = \{\bar{x} \mid (\exists v_1)(\forall v_2) .. (Q v_m)(Q v_{m+1}) P_1(x_1 .. x_k, v_1 .. v_m v_{m+1})\}$

$A \in \Pi_{m+1}$ $\quad \bar{A} = \{\bar{x} \mid (\forall v_1)(\exists v_2) ... (Q v_m)(Q v_{m+1}) P_1(x_1 .. x_k, v_1 .. v_m v_{m+1})\}$

(g) $A \leq_m B$, $B \in \Sigma_m \Rightarrow A \in \Sigma_m$

$(\forall x \in N)$ $\quad x \in A \Leftrightarrow f(x) \in B$

$B = \{x \mid (\exists v_1) ... (Q v_m) P(x, v_1 .. v_m)\}$

$A = \{x \mid (\exists v_1) .. (Q v_m) P(f(x), v_1 .. v_m)\}$

a)
c) } jedným razom indukciou
d)

d) $\exists v\, P(\bar{x}, y, v)$ je Σ_m podmienka
pridáme ohraničený kvantifikátor:
$\exists y < z\ \exists v\, P(\bar{x}, y, v) \iff \exists v\ \exists y < z\, P(\bar{x}, y, v)$ *
$\forall y < z\ \exists v\, P(\bar{x}, y, v) \iff \exists w\ \forall y < z\ \exists v < w\, P(\bar{x}, y, v)$ **

* $\exists v (\exists y < z\, (P(\bar{x}, y, z)))$ VR $m = 1$
$\in \Pi_{m-1}$ $m \geq 2$
využijeme ind. predpoklad

** $\exists w (\forall y < z\ \exists v < w\, P(\bar{x}, y, v))$

Aritmetická hierarchia:

Aritmetická hierarchia:

$\text{VRM} \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \Sigma_3 \subseteq \cdots$
$\text{VRM} \subseteq \Pi_1 \subseteq \Pi_1 \subseteq \Pi_3 \subseteq \cdots$
$\Sigma_i \subseteq \Pi_{i+1}$
$\Pi_i \subseteq \Sigma_{i+1}$

Lema 9.1.1 *(Podozrenie o možnom kolapse hierarchie) Ak $\Sigma_n \subseteq Pi_n$ alebo $\Pi_n \subseteq \Sigma_n$. Potom pre každé $m \geq n$ platí vzťah $\Sigma_m = \Pi_m = \Sigma_n$.*

Dôkaz. a) Ukážeme $\Pi_n = \Sigma_n$. (z predpokladu, že $\Sigma_n \subseteq \Pi_n$, tak $\Pi_n \subseteq \Sigma_n$).
Ak $A \in \Pi_n$, potom $\bar{A} \in \Sigma_n$, potom $\bar{A} \in \Pi_n$, potom $A \in \Sigma_n$.

b) Ukážeme, že $\Sigma_{n+1} \subseteq \Sigma n$. $A = \{\bar{x} | (\exists v) P(\bar{x}, v)\}$.
$P(\bar{x}, v) \in \Pi_n = \Sigma_n$. Pridanie existenčného kvantifikátora to nezmení, bude stále v Σ_n.

c) $\Pi_{n+1} \subseteq Pi_n$.

d) – stačí spraviť indukciu

Definícia. Množina $B \subseteq \mathbb{N}$ je Σ_n-kompletná ak $B \in \Sigma_n \wedge (\forall A)(A \in \Sigma_n \Rightarrow A \leq_m B)$.
Množina $B \subseteq \mathbb{N}$ je Π_n-kompletná ak $B \in \Pi_n \wedge (\forall A)(A \in \Pi_n \Rightarrow A \leq_m B)$.
Relácia $Q \subseteq \mathbb{N}^2$ je Σ_n-univerzálna ak $Q \in \Sigma_n$ a $(\forall A)(A \subseteq \mathbb{N} \wedge A \in \Sigma_n \Rightarrow (\exists a)(A = \{v | Q(a|v)\}))$
Relácia $Q \subseteq \mathbb{N}^2$ je Π_n-univerzálna ak $Q \in \Pi_n$ a $(\forall A)(A \subseteq \mathbb{N} \wedge A \in \Pi_n \Rightarrow (\exists a)(A = \{v | Q(a|v)\}))$

Definícia. $Q_1 = \{(x, v) | v \in W_x\} = \{(x, v) | \Phi_x(v)$ je definované $\}$.
$Q_{n+1} = \{(x, v) | (\exists y)(Q_n(x, c(v, y)))\}$
$H_n = \{c(x, v) | Q_n(x, v)\}$
$D_n = \{x | Q_n(x, x)\}$

Poznámka. $H_1 = K_0 = \{c(x, v) | v \in W_x\}$
$D_1 = K = \{x | x \in W_x\}$
Indukciou sa dá dokázať, že $Q_n \in \Sigma_n$.
Dokaz:

1. $Q_1 = \{(x, v) | v \in W_x\}$. Je to definičný obor nejakého algoritmu, $\Phi_x(v)$ je definovaná. – ROM – $= \{(x, v) | (\exists y) T(x, v, y)\} i$ – je to Σ_1

2. $Q_{n+1} = \{(x, v) | (\exists y)(T(x, v, y))\}$. Zoberieme to, znegujeme, kvantifikatory sa otocia, negacia sa otocia, a teda to patri do Σ_{n+1}. Preto aj $H_n \in \Sigma_n$ a $D_n \in \Sigma_n$.

Veta 9.1.2

1. *Každé* Q_n *je* Σ_n*-univerzálna a doplnok je* Π_n*-univerzálny.*
2. H_n *je* Σ_n*-kompletná,* $\bar{H}_n$ *je* Π_n *kompletná.*
3. $D_n \in \Sigma_n \backslash \Pi_n$ *a* $\bar{D}_n \in \Pi_n \backslash \Sigma_n$.

Veta 9.1.3 $(S - m - n)$
Pre každú dvojicu nenulových čísiel n *a* m *existuje všeobecne rekurzívna funkcia* $S_n^m \in VRF^{(n+1)}$ *taká, že pre každé* $e, x_1, \ldots, x_n$ *platí:*

$$\Phi^{(m)}_{S_n^m(e,x_1,\ldots,x_n)} = \lambda v_1, \ldots, v_m(\Phi_e^{n+m}(x_1, \ldots, x_n, v_1, \ldots, v_m)$$

Dôkaz. e – číslo programu P – načítava $n + m$ vstupných hodnôt. P' – program, ktorý miesto načítavanie $x_1, \ldots, x_n$ bude ich mať v sebe zapísané. Potom podľa church tézy to platí.

Veta 9.1.4

(a) *Nech* $\Psi \in RF^{(n+m)}$. *Potom existuje* $g \in VRF^{(n)}$, *ktorá pre každé* $x_1, \ldots, x_n$ *spĺňa* $\Phi^{(m)}_{g(x_1,\ldots,x_n)} = \lambda v_1, \ldots, v_m \Psi(x_1, \ldots, x_n, v_1, \ldots, v_m)$.

(b) *Nech* $Q \in ROM^{(n+m)}$ *je relácia. Potom existuje taká* $g \in VRF^{(n)}$, *ktorá pre každé* $x_1, \ldots, x_n$ *spĺňa* $W^{(m)}_{g(x_1,\ldots x_n)} = \{v_1, \ldots, v_m | Q(x_1, \ldots, x_n, v_1, \ldots, v_m\}$.

Príklad. $Unb = \{x | W_x$ je nekonečná $\}$.

Riešenie. W_x je nekonečná $\Leftrightarrow (\forall v_1)(\exists v_2)(v_1 < v_2 \wedge v_2 \in W_x)$
Poznámka – $\Phi_x(v_2)$ je definovaná.
Platí: $\Sigma_1 = ROM$
$v_1 < v_2$ – primitívne rekurzívne.
$v_2 \in W_x$ – byť v definičnom obore, to nie je VRM, ale ROM
$min(y, T(e, x_1, \ldots, x_n, y)$ – ak $(\exists y)T(e, x_1, \ldots, x_n, y)$
T je PR
konjukcia – je ROM
Pridám existenčný kvantifikátor – je to uzavreté, stále ROM.
Pridáv všeobecný – je to potom Π_2

Príklad. $Rec = \{x | W_x$ je všeobecne rekurzívna $\}$

Dôkaz. W_x je rekurzívna $\Leftrightarrow (\exists y)(W_y = \bar{W}_x) \Leftrightarrow (\exists y)(\forall v)((v \in W_y \wedge v \notin W_x) \vee (v \notin W_y \wedge v \in W_x))$
$(v \in W_y)$ je ROM.
$(v \notin W_x)$ podľa (c),(f) $\Rightarrow$ je konjukcia v $\Sigma_2 \cap \Pi_w$. Druhý kus toho tam tiež patrí, $\vee$ to nezmení.
Všeobecný kvantifikátor to dá na Π_2 a existenčný na Σ_3.

Príklad. Totálnosť $Tot =^{def} \{x | \Phi_x$ je totálna $\}$.
Cieľ: ukážeme, že Tot je Π_2-kompletná.

a) $Tot \in \Pi_2$ – $e \in Tot \Leftrightarrow (\forall v)(\exists y)(T(e, v, y) = 0)$

b) Ukážeme, že $(\forall A)(A \in \Pi_2 \Rightarrow A \leq_m Tot)$.
Nech $A \subseteq \mathbb{N}$ je ľubovoľná Π_2 množina.
$A = \{x | (\forall v)(\exists y)R(x, v, y)\}$
$x \in A \Leftrightarrow (\forall v)(\exists y)R(n, v, y)$.
$\Psi(x, v) =^{def} \lambda v(min(y, R(x, v, y))) \in$ČRF
Konštanta $x \in A \rightarrow \Psi(x, v)$ je totálna
Konštanta $x \notin A \rightarrow \Psi(x, v)$ nie je totálna
$\Psi(x, v) = \Phi_{g(x)}(v)$, t.j. $g(x)$ (je VRF) je index funkcie $\Phi(x, v)$.
$x \in A \Leftrightarrow \Phi_{g(x)}(v)$ je totálna funkcia $\Leftrightarrow g(x) \in Tot$.

Príklad. Niekde definované funkcie.

$B =^{def} \{x | W_x \neq \emptyset\} = \{x | (\exists y) y \in W_x\}$.

a) $B \in \Sigma_1$.

b) $(\forall A \in \Sigma_1)(A \leq_m B)$. Nech A je ľubovoľná ROM. Nech $Q_A =^{def} \{(x, v) | x \in A\} = A \times \mathbb{N}$ Q_A je ROM.

Ak $x \in A \rightarrow \{v | (x, v) \in Q_A\} = \mathbb{N}$

Ak $x \notin A \rightarrow \{v | (x, v) \in Q_A\} = \emptyset$

$x \in A \Leftrightarrow W_{g(x)} \neq \emptyset$. – dokonči si to ($S - m - n$ veta)

$t.j. A \leq_m B \Rightarrow B$ je Σ_1-kompletná $\Rightarrow B \notin VRM, \bar{B} \notin ROM.$.

5. Modely vypočítateľnosti (Turingove stroje a iné modely).

Veta 8.45. Pre každý registrový stroj Z a každé $n \in \mathbb{N}$ existuje taký Turingov stroj T, že $\Phi_Z^n = \Phi_T^n$.

Dôkaz: Nech Q je množina všetkých vnútorných stavov v M-inštrukciách stroja Z a nech q_u, q_v $(u < v)$ sú vnútorné stavy s najnižšími indexmi, ktoré nepatria do množiny $Q \cup \{q_0, q_1\}$. Označme Z' stroj, ktorý vznikne zo Z nahradením q_1, q_0 symbolmi q_u, q_v. Každej M-inštrukcii X stroja Z' priraďme Turingov stroj T_X tak, aby boli splnené nasledujúce podmienky:

(1) Ak $X = (q_i S_j P q_k)$ alebo $X = (q_i S_j M q_k)$, tak existuje jediná inštrukcia stroja T_X, ktorá sa začína q_i, a jediná inštrukcia T-stroja T_X, ktorá sa končí q_k. Žiadne ďalšie T-inštrukcie stroja T_X neobsahujú vnútorné stavy z množiny $Q \cup \{q_0, q_1, q_u, q_v\}$.

(2) Ak $X = (q_i S_j q_r q_s)$, tak existuje jediná T-inštrukcia stroja T_X začínajúca sa q_i, jediná jeho T-inštrukcia končiaca sa q_r a jediná jeho T-inštrukcia končiaca sa q_s. Okrem týchto výnimiek neobsahujú T-inštrukcie stroja T_X vnútorné stavy z množiny $Q \cup \{q_0, q_1, q_u, q_v\}$.

(3) Žiaden vnútorný stav, ktorý nepatrí do množiny $Q \cup \{q_0, q_1, q_u, q_v\}$, sa nenachádza v inštrukciách dvoch strojov T_X, T_Y pre $X \neq Y$.

(4) Ak $X = (q_i S_j P q_k)$, resp. $X = (q_i S_j M q_k)$, tak pre každé $m \geq j$ a všetky $k_0, \ldots, k_m \in \mathbb{N}$ platí

$$\begin{aligned} q_i \operatorname{Slv}(k_0, \ldots, k_{j-1}, k_j, k_{j+1}, \ldots, k_m) &\overset{T_X}{\Longmapsto} \\ \overset{T_X}{\Longmapsto}\ q_k \operatorname{Slv}(k_0, \ldots, k_{j-1}, k_j + 1, k_{j+1}, \ldots, k_m) \end{aligned} \tag{8.45.1}$$

resp.

$$\begin{aligned} q_i \operatorname{Slv}(k_0, \ldots, k_{j-1}, k_j, k_{j+1}, \ldots, k_m) &\overset{T_X}{\Longmapsto} \\ \overset{T_X}{\Longmapsto}\ q_k \operatorname{Slv}(k_0, \ldots, k_{j-1}, k_j - 1, k_{j+1}, \ldots, k_m) \end{aligned} \tag{8.45.2}$$

(5) Ak $X = (q_i S_j q_r q_s)$, tak pre každé $m \geq j$ a všetky $k_0, \ldots, k_m \in \mathbb{N}$ platia vzťahy

$$\begin{aligned} q_i \operatorname{Slv}(k_0, \ldots, k_{j-1}, 0, k_{j+1}, \ldots, k_m) &\overset{T_X}{\Longmapsto} \\ \overset{T_X}{\Longmapsto}\ q_s \operatorname{Slv}(k_0, \ldots, k_{j-1}, 0, k_{j+1}, \ldots, k_m) \end{aligned} \tag{8.45.3}$$

$$\begin{aligned} q_i \operatorname{Slv}(k_0, \ldots, k_{j-1}, k_j + 1, k_{j+1}, \ldots, k_m) &\overset{T_X}{\Longmapsto} \\ \overset{T_X}{\Longmapsto}\ q_r \operatorname{Slv}(k_0, \ldots, k_{j-1}, k_j + 1, k_{j+1}, \ldots, k_m) \end{aligned} \tag{8.45.4}$$

Teraz vytvorme Turingov stroj T' ako množinové zjednotenie všetkých T-strojov T_X:

$$T' = \bigcup \{T_X | X \in Z'\} \tag{8.45.5}$$

Turingov stroj T' má nasledujúcu vlastnosť: Ak m je prirodzené číslo väčšie alebo rovnajúce sa najväčšiemu indexu registrov R_i v inštrukciách M-stroja Z', tak pre všetky $r_0, r_1, \ldots, r_m$, $s_0, s_1, \ldots, s_m \in \mathbb{N}$ a všetky $q_i, q_j \in (Q \setminus \{q_0, q_1\}) \cup \{q_u, q_v\}$ platí

$$(q_i; r_0, r_1, \ldots, r_m) \overset{Z'}{\Longmapsto} (q_j; s_0, s_1, \ldots, s_m) \tag{8.45.6}$$

práve vtedy, keď

$$q_i \operatorname{Slv}(r_0, r_1, \ldots, r_m) \overset{T'}{\Longmapsto} q_j \operatorname{Slv}(s_0, s_1, \ldots, s_m) \tag{8.45.7}$$

Nech teraz m' je maximálny index registra v M-inštrukciách stroja Z (ak $Z = \emptyset$, položíme $m' = 0$) a $m = \max(m', n)$. Nájdime také T-stroje T_1, T_2, že

(1) T_1 obsahuje jedinú inštrukciu začínajúcu sa q_1 a jedinú inštrukciu končiacu sa q_u. T_2 obsahuje jedinú inštrukciu začínajúcu sa q_v a jedinú inštrukciu končiacu sa q_0. Okrem týchto výnimiek neobsahujú inštrukcie strojov T_1, T_2, T' žiadne rovnaké vnútorné stavy.

(2) pre všetky $k_0, k_1, \ldots, k_n \in \mathbb{N}$ platí

$$q_1 \operatorname{Slv}(k_1, \ldots, k_n) \overset{T_1}{\Longmapsto} q_u \operatorname{Slv}(0, k_1, \ldots, k_n, \underbrace{0, \ldots, 0}_{m-n})$$

(3) pre každé $r \in \mathbb{N}$, a $k_0, k_1, \ldots, k_r \in \mathbb{N}$

$$q_v \operatorname{Slv}(k_0, k_1, \ldots, k_r) \overset{T_2}{\Longmapsto} q_0 \operatorname{Slv}(k_0) \tag{8.45.8}$$

Teraz už môžeme vytvoriť stroj T:

$$T = T' \cup T_1 \cup T_2 \tag{8.45.9}$$

Dôkaz rovnosti $\Phi_Z^n = \Phi_T^n$ prenechávame čitateľovi ako cvičenie. □

6. Ekvivalentnosť modelov vypočítateľnosti.

Veta 7.0.2 *a)* $A \nsubseteq \mathbb{N} \Rightarrow \emptyset \leq_m A$

b) $\emptyset \neq A \subseteq \mathbb{N} \Rightarrow \mathbb{N} \leq_m A$

c) $\emptyset \nleq_m \mathbb{N}$ *a* $\mathbb{N} \nleq_m \emptyset$

d) $A =_m \emptyset \Rightarrow A = \emptyset$

e) $A =_m \mathbb{N} \Rightarrow A = \mathbb{N}$

f) $\emptyset \nsubseteq A, B \nsubseteq$ *a* A, B *sú všeobecne rekurzívne množiny, potom* $A =_m B$

g) $A, B \subseteq \mathbb{N}, A \leq_m B$, B *je všeobecne rekurzívna množina, potom* A *je všeobecne rekurzívna množina.*

h) A *je všeobecne rekurzívna,* B *je rekurzívne očíslovateľná, ale nie je všeobecne rekurzívna, potom* $A \leq_m B, A \neq_m B$.

i) Všeobecne rekurzívne množiny tvoria 3 triedy ekvivalencie

Veta 4.0.5 *Existuje prostá množina.*

Dôkaz. Potrebujeme zostrojiť $S \subseteq \mathbb{N}$ a jej doplnok $\bar{S}$.

S je rekurzívne očíslovateľná.

$\bar{S}$ je imúnna množina – je nekonečná, neobsahuje rekurzívne očíslovateľné podmnožiny.

Stačí: do S dáme aspoň jeden prvok z každej nekonečnej rekurzívne očíslovateľnej množiny ale tak, aby mimo S ostalo nekonečne veľa prvkov. Napríklad: Z množiny číslo i vyberieme prvok s veľkosťou aspoň $2i$.

W – univerzálna množina?

Nech $T = \{(i,x) | (x \in w_i) \wedge (x > 2i)\} = W \cap \{(i,x) | (x > 2i)\}$

W – rekurzívne očíslovateľná množina, $\{(i,x)|(x > 2i)\}i$ je rekurzívna množina – aj očíslovateľná, čiže prienik je tiež rekurzívne očíslovateľná množina.

Pri generovaní monžiny T budeme odhadzovať tie dvojice (i,x), ktorého prvý člen i sme už „stretli". Z každého w_i spravíme jedno číslo (ak w_i je nekonečné).

Takto vygenerujeme množinu T'. S je projekcia množiny T'.

S je rekurzívne očíslovateľná množina, má spoločný prvok s každou nekonečnou rekurzívne očíslovateľnou množinou a $\bar{S}$ je nekonečná množina, lebo z prvých i množín sme vybrali maximálne i prvkov a aspoň i prvkov ostalo.

Definícia. Budeme hovoriť, že množina je imúnna, ak je nekonečná a neobsahuje nekonečné rekurzívne očíslovateľné podmnožiny (Rekurzívne očíslovateľná množina sa nazýva prostou, ak jej doplnok je imúnny).

Poznámka. Prostá funkcia nemôže byť rekurzívna (Postova veta).